UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,092	10/03/2003	David Andrew Thomas	200309084-1	3543

22879 7590 09/21/2011

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2432	

NOTIFICATION DATE	DELIVERY MODE
09/21/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVID ANDREW THOMAS, PUNEET SHARMA,
SUJATA BANERJEE, SUNG-JU LEE,
and AMY CSIZMAR DALAL

Appeal 2009-011256
Application 10/679,092
Technology Center 2400

Before ERIC S. FRAHM, KRISTEN L. DROESCH, and
DENISE M. POTHIER, *Administrative Patent Judges*.

POTHIER, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-10, 12-17, 20, 22, 23, and 26. Claims 18, 19, 24, 25, and 30 have been withdrawn from consideration (Br. 3), and the Examiner has withdrawn the rejection of claims 11, 21, and 27-29 (Ans. 2). We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

STATEMENT OF THE CASE

Appellants' invention relates to a technique for downloading content to a remote device over both insecure and secure communication channels. *See generally* Spec. 2:10-21. Claim 1 is reproduced below with key disputed limitations emphasized:

> 1. (Original) A method for facilitating content downloads via an insecure communications channel, comprising:
>
> *receiving from a device via an insecure communications channel at least one shared secret in encoded form* that functions as an identifier of the device;
>
> transmitting encrypted content via the insecure communications channel from a content server to the device;
>
> *receiving the shared secret in plaintext form* via a secure communications channel;
>
> receiving a confirmation authorizing release of a decryption key; and
>
> sending the decryption key for decryption of the encrypted content.

The Examiner relies on the following as evidence of unpatentability:

Katayama	US 2002/0027994 A1	Mar. 7, 2002
Wiser	US 6,385,596 B1	May 7, 2002
Parenty	US 2002/0064283 A1	May 30, 2002

THE REJECTIONS

1. The Examiner rejected claims 1-10, 12-17, 22, and 23 under 35 U.S.C. § 103(a) as unpatentable over Wiser and Parenty. Ans. 3-6.[1]

2. The Examiner rejected claims 20 and 26 under 35 U.S.C. § 103(a) as unpatentable over Wiser, Parenty, and Katayama. Ans. 6-8.

---

[1] Throughout this opinion, we refer to (1) the Appeal Brief filed November 4, 2008 and (2) the Examiner's Answer mailed March 2, 2009.

Initially, we consider Appellants' assertions that the Examiner's objection to the Specification related to the phrase, "tangible computer readable medium" in claims 22 and should be reversed. *See* Br. 10. Such issues are petitionable matters under 37 C.F.R. § 1.181 and will not be addressed on appeal. *See* MPEP §§ 1002 and 1201. We next turn the art rejections.

THE OBVIOUSNESS REJECTION OVER WISER AND PARENTY

Regarding independent claim 1, the Examiner finds that Wiser teaches receiving a shared secret (e.g., a credit card number) from a client system (e.g., 126) through an insecure communications channel over the Internet and a Secure Socket Layer (SSL). Ans. 3. The Examiner contends that SSL is a protocol used on the Internet to secure transmissions and does not create a secure channel but securely transmits over an insecure channel. Ans. 9. Appellants argue that using SSL makes a channel secure, as evidenced by the Background of the Invention and Parenty. Br. 12.

The Examiner also finds that Wiser teaches transmitting the shared secret information in an encoded form through an insecure channel (Ans. 3) and then transmitting this information to the payment processor (Ans. 3-4, 9). The Examiner relies on Parenty in combination with Wiser to teach and suggest transmitting the shared secret over a secure channel in plaintext form to the payment processor. Ans. 4, 9. Appellants contend that Wiser and Parenty fail to teach or suggest receiving the shared secret twice and in two forms -- (1) an encoded form and (2) a plaintext form. *See* Br. 13.

ISSUES

(1) Under § 103, has the Examiner erred in rejecting claim 1 by finding that Wiser and Parenty collectively would have taught or suggested "receiving from a device via an insecure communications channel at least one shared secret" giving the term "an insecure communications channel" its broadest reasonable interpretation in light of the Specification?

(2) Under § 103, has Examiner erred in rejecting claim 1 by finding that Wiser and Parenty collectively would have taught or suggested also receiving the shared secret both in encoded and plaintext form?

FINDINGS OF FACT (FF)

1. Appellants' Specification discloses that "[t]he wireless communication channel 5 is presumed to be an insecure channel because it is vulnerable to intruder's snooping." Spec. 4:30-5:1; Fig. 1.

2. Appellants' Specification also discloses that "the secure channel 7 may be established through a land-line[,] such as a telephone wire, or underground cabling . . . [that] offers additional protection against third parties who may be attempting to capture the communication by snooping." Spec. 6:28-31; Fig. 1.

3. Wiser discloses transmitting music and related media over a public telecommunications network, such as the Internet. The system employs client-server architecture and includes: a client system 126 having a media player 116 and a Web browser 128; a music distribution center 124 having a HyperText Transfer Protocol (HTTP) server 122; and a media licensing center 110 interfacing with the music distribution center 124. Col. 5, ll. 43-60; Figs. 1A-B.

4. During registration, Wiser's system collects personal information (e.g., a credit card number) and transmits the information from the client's Web browser 128 to media licensing center 110 at step 610, preferably over a secure link, such as using SSL v.3. Col. 13, ll. 6-27; Figs. 1, 6A.

5. Wiser's media licensing center 110 extracts the credit card information during registration and verifies the information by requesting credit card authorization at 612 from the payment processor 134. During purchase, the credit card number and form data at steps 912 and 914 is passed to servers 122 and 132. Col. 11, ll. 26-38, 46-48; col. 13, ll. 28-30; col. 16, ll. 53-65; Figs. 1A-B, 6A, 9AA-9AB.

6. Parenty teaches known computing platforms, including laptops, personal data assistants (PDAs), and cellular phones. ¶ 0028.

7. Parenty teaches clear text private and symmetric keys can be transmitted over secure channels with confidentiality. Parent also teaches using physical protection measures to secure channels. ¶ 0033.

ANALYSIS

We begin by construing the key disputed limitation of claim 1 which calls for, in pertinent part, "an insecure communications channel . . . ." Notably, all communication channels are vulnerable to attack (e.g., snooping, phishing, physically obtaining passwords) and are never completely "secure." As such, some communication channels are at best more secure than others. That being said, the Examiner and Appellants disagree on whether Wiser's disclosed communication channel, which preferably uses a SSL protocol to send personal information over a network (*see* FF 3-4), is an insecure or secure communication channel. In light of

Appellants' disclosure, the phrase, "an insecure communication channel," however, encompasses a different meaning or construction.

Appellants have disclosed that an insecure communication channel includes a wireless communication channel (*see* FF 1), and a secure communication channel includes land-line communications (*see* FF 2). Also, when discussing combining Parenty with Wiser, the Examiner takes the position that a secure channel is "a hard wired channel[.]" *See* Ans. 9. Thus, we find that the insecure communication channel recited in claim 1 includes a wireless communication channel, given its broadest reasonable construction in light of the disclosure. Wiser discloses transmitting information in the system between the client (e.g., 126) and the server (e.g., 110, 124) over a public network, such as the Internet. FF 3. While Wiser does not provide further details about the network, Wiser's reference to a public network suggests that the transmission can be either wired or wireless. Furthermore, we take judicial notice[2] of the fact that an ordinarily skilled artisan would have recognized that Wiser's public network could be wireless and thus includes an insecure communications channel.

Moreover, Wiser discloses the client (e.g., 126) includes a Web browser 128 (*see* FF 3) but provides no examples of the client device. Parenty teaches some known computing platforms, such as laptops, PDAs, and cellular phones (*see* FF 6), which are known by an ordinarily skilled artisan to include web browsers and to transmit information over wireless channels. Therefore, despite Wiser's discussion of transmitting information

---

[2] *See In re Ahlert*, 424 F.2d 1088, 1091 (CCPA 1970) (explaining that "the Patent Office appellate tribunals, where it is found necessary, may take notice of facts beyond the record which, while not generally notorious, are capable of such instant and unquestionable demonstration to defy dispute.")

over a secure link (*see* FF 4), we conclude that Wiser and Parenty collectively teach and suggest receiving information from a device (e.g., a client system's device) (*see* FF 3, 4, 6) through "an insecure communications channel" because the phrase is broadly construed to include wireless communications.

Wiser also discloses transmitting a credit card number (e.g., a shared secret) between the client and server system using SSL v.3. *See* FF 3-4. According to Microsoft Computer Dictionary, SSL "supports authentication of client, server, or both, as well as encryption during a communications session."[3] Thus, in combination with the above discussion of how the cited references suggest transmitting information over an insecure communications channel, Wiser further suggest this insecure communications channel receives a shared secret in encoded form from a client system or device as recited. Wiser's technique therefore first forwards the registration or shared secret information (e.g., credit card number) from the client system 126 (e.g., a device) to the media licensing center 110 (*see* FF 3-4) and is a first step of receiving the shared secret in a first or encoded form.

Notably, the second limitation of "receiving the shared secret in a plaintext form" does not recite which device or component receives the shared secret. Thus, contrary to Appellants' contentions (*see* Br. 13), this receiving step does not require that *the media licensing center* receives the shared secret. After Wiser's media licensing center 110 receives the credit card information or shared secret (FF 4), the center 110 then forwards the credit card number to the payment processor 134 or receives the shared

[3] See *Microsoft® Computer Dictionary* 495 (5th ed. 2002).

secret for a second time (*see* FF 5). While Wiser does not teach in what form this information is received, Parenty teaches and suggests that sensitive information can be transmitted in a clear text format over secure channels with confidentiality using physical measures. *See* FF 7. The Examiner also notes an example of physical measures, such as a hard-wired channel. *See* Ans. 3-4, 12. Thus, combining this teaching with Wiser's use of sensitive information (e.g., a credit card number) yields no more than one would expect from such an arrangement. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 416-17 (Fed. Cir. 2007). That is, the combination predictably yields a technique for transmitting a shared secret (e.g., a credit card number) in a plaintext form over a secure communications channel on the server side to ensure confidentiality remains. *See* FF 5, 7.

For the foregoing reasons, Appellants have not persuaded us of error in the obviousness rejection of: independent claim 1 and claims 2-10, 12-17, 22,[4] and 23 not separately argued with particularity (Br. 12-14).

THE OBVIOUSNESS REJECTION OVER WISER, PARENTY, AND KATAYAMA

Regarding representative claim 20, the Examiner finds that Wiser teaches receiving a confirmation authorizing release of a decryption key upon verifying a purchase voucher, but that neither Wiser nor Parenty teaches prompting the user to accept terms of download and decryption of the encrypted content after successfully downloading encrypted content from a content server. *See* Ans. 7-8. The Examiner relies on Katayama to

[4] When arguing independent claim 22, Appellants refer to claim 1 and repeat the argument made for claim 1 -- Wiser and Parenty do not teach or suggest receiving a shared secret twice and in two forms. *See* Br. 13. We therefore group claim 22 with claim 1. *See* 37 C.F.R. § 41.37(c)(1)(vii).

cure this deficiency and to provide a reason for combining with Wiser. Ans. 8.

Citing to column 8, lines 19-32, Appellants argue that Wiser teaches purchasing the media file prior to downloading the file. Br. 15. Because the purchase is purportedly already made, Appellants then assert that the Examiner has not provided an adequate reason in Wiser to repurchase the file and thus combine Katayama's teaching with Wiser. *See id.*

ISSUE

Under § 103, has the Examiner erred in rejecting claim 20 by finding that Wiser, Parenty, and Katayama collectively would have taught or suggested prompting the user to accept download terms, after receiving confirmation of a successful encrypted content download from the content server?

ADDITIONAL FINDINGS OF FACT

8. Wiser discusses a media voucher is an object used to control the purchase and preview of media data files 200. For each preview or purchase, a new media voucher is created. Col. 8, ll. 19-32; Figs. 2-3.

9. Prior to purchase, Wiser's Figure 7 shows the process 700 of previewing a media data file 200. A media voucher 300 is sent to the client's web browser 128. Preview enables the user to decide whether or not to purchase a song. Col. 11, ll. 39-48; Col. 14, ll. 37-39; col. 15, ll. 19-28; Figs. 1A-B, 2, and 7A-B.

10. Katayama teaches providing a low sound quality audio to a consumer using a first key so the user can perform sample playback of audio

content before deciding whether to buy a second key that provides a high quality audio content. This technique prevents illegal use and copying of high sound quality audio content. ¶¶ 0008-0009, 0089.

11. Katayama teaches the transceiver 112 lets the consumer know that the second key is needed and urges the consumer to buy the key if the second key 120 for the watermark embedded signal 203 is not found when extracting means 117 searches storage 114. ¶ 0063-64; Fig. 1.

ANALYSIS

Based on the record before us, we find no error in the Examiner's rejection. We disagree that Wiser teaches at column 8, lines 19-32 purchasing the media file prior to downloading a media file. Rather, Wiser discusses a media voucher which is used to control the purchase and preview of media files. *See* FF 8. Figure 7 shows the process 700 of previewing a media data file 200 that sends a media voucher to the client *prior to purchase*. FF 9. Another media voucher is created when purchasing the media file. *See* FF 8.

Also, as the Examiner indicates (Ans. 7-8, 10), the rejection of claim 20 is not based solely on Wiser but Wiser, as modified by Katayama's teaching. Katayama teaches providing the user with a degrading, lower-quality audio content to sample or preview content with a first key prior to the user purchasing a higher quality audio content with a second key to prevent illegal use and copying of high sound quality audio content. *See* FF 10. Thus, combining Katayama's teaching (*see id.*) with Wiser's previewing technique prior to purchasing yields no more than an ordinarily skilled artisan would expect or predictably yields a system that permits a user to

preview lower-quality media content before prompting the user to accept download terms (e.g., prior to purchase) for a higher-quality audio content. *See KSR*, 550 U.S. at 416-17. Such a modification would not destroy Wiser's function of previewing content prior to purchase and preventing illegal use (*see* FF 10).

Moreover, Katayama's encrypted audio file has been downloaded to the user (e.g., the watermark embedded signal 203), as indicated by the user only needing the key to listen to the higher-quality audio file. *See* FF 10-11. That is, Katayama teaches notifying the consumer that a second key (e.g., 120) is needed to obtain the higher-quality audio and urges the consumer to purchase the key. *See* FF 11. This notification serves as confirmation of successfully downloading an encrypted content from the content server. *See id*. Thus, Katayama teaches the user is prompted to purchase the second key or accept the terms of the download, after the confirmation of successfully downloading encrypted content. *See id*. We also refer to the Examiner's discussion (*see* Ans. 8, 10) and conclude that Wiser in combination with Parenty and Katayama teaches or suggests prompting the user to accept download terms, after receiving confirmation of a successful encrypted content download from the content server as recited in claim 20.

For the foregoing reasons, Appellants have not persuaded us of error in the obviousness rejection of independent claim 20 and claim 26 not separately argued with particularity (Br. 14-15).

CONCLUSION

Under § 103, the Examiner did not err in rejecting claims 1-10, 12-17, 20, 22, 23, and 26.

DECISION

The Examiner's decision rejecting claims 1-10, 12-17, 20, 22, 23, and 26 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

ke

EVIDENCE

Microsoft® Computer Dictionary 495 (5th ed. 2002).